PROGRAM MATERIALS
Program #2951
June 27, 2019

GDPR- A Guide for Corporate Counsel (What They Need to Know to Advise Their Clients)

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

BRYAN CAVE LEIGHTON PAISNER BCLP

GDPR
- A Guide For Corporate Counsel -

Chair Data Privacy and Security Team
David Zetoony, David.Zetoony@bclplaw.com

bclplaw.com

Agenda

Agenda

Level 1: The 30 second elevator speech to executives.

Level 2: Historical context.

Level 3: Core worldview: “processors” and “controllers.”

Level 4: What does it actually require.

Level 5: Core compliance documents

- **5(1): Data Inventories**
- **5(2): Retention Policies**
- **5(3): Information Notices**
- **5(4): Data Subject Request Protocols**
- **5(5): Data Protection Impact Assessments**
- **5(6): Written Information Security Plans**
- **5(7): Data protection Officer**
- **5(8): Incident Response Plan**
- **5(9): Cross Border Transfers**
- **5(10): Third Party Vendor Management**

Level 1: 30 second elevator speech for executives

1. Extraterritorial. Purports to impact "establishments" in the EU and other organizations that monitor behavior of Europeans or offer services to people in Europe
2. Penalties. Up to 4% of gross revenue for some violations.
3. Right of access. People have the right to request access to the information that you keep about them.
4. Right to be forgotten / rectification. People have the right to have information about them erased or corrected.
5. Record keeping requirements. Requires that personal data be kept for no longer than is necessary.

Level 2: Historical context

Level 2: Historical context

- The EU Data Protection Directive (EC/46/95)
  - Enacted in 1995
  - Creates a standard legal *framework* for EU member states.
  - It was not a self-implemented statute, regulation, or rule.
  - In US legal parlance, it was akin to an unfunded federal mandate.
  - There were 28 state implementing statutes in various languages, with various texts, and with various requirements.
  - There is an advisory body (the Article 29 Working Party) that provided interpretative guidance.

Level 2: Historical context

The General Data Protection Regulation (EU) 2016/679

- Replaces the EU Data Protection Directive.
- Entered into force on May 2016,
- Applied beginning May 2018,
- Directly applicable in all EU Member States,
- Aims to unify data protection law within the European Union and increases data subject's rights,
- Still authorizes individual EU Member States to implement more specific rules in certain areas.

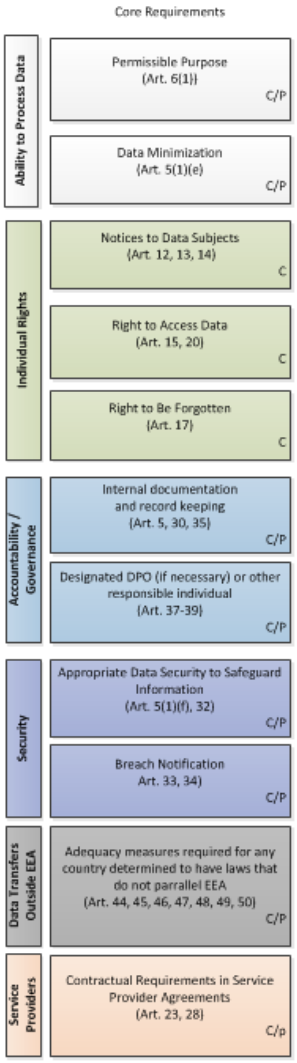
Level 3: Core worldview “processors” and “controllers.”

Requirements differ depending upon whether you are a “Data Controller” or a “Data Processor.”

- A “Data Controller” is defined as the entity which “determines the purposes and means of the processing of personal data.” GDPR, Art. 4(7).

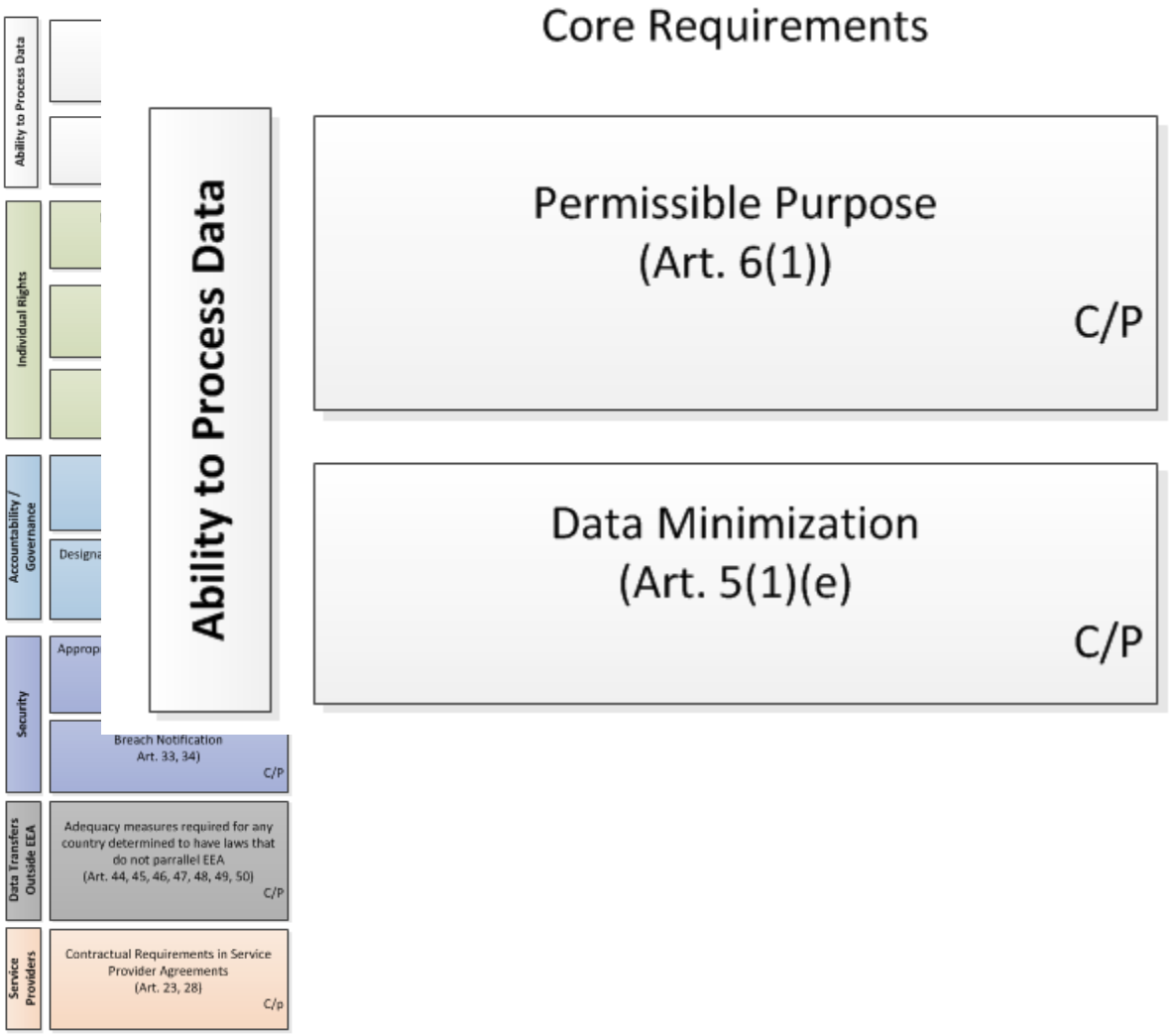
- A “Data Processor” is defined as an entity “which processes personal data on behalf of the controller.” GDPR, Art. 4(8).

Level 4: What does it actually require



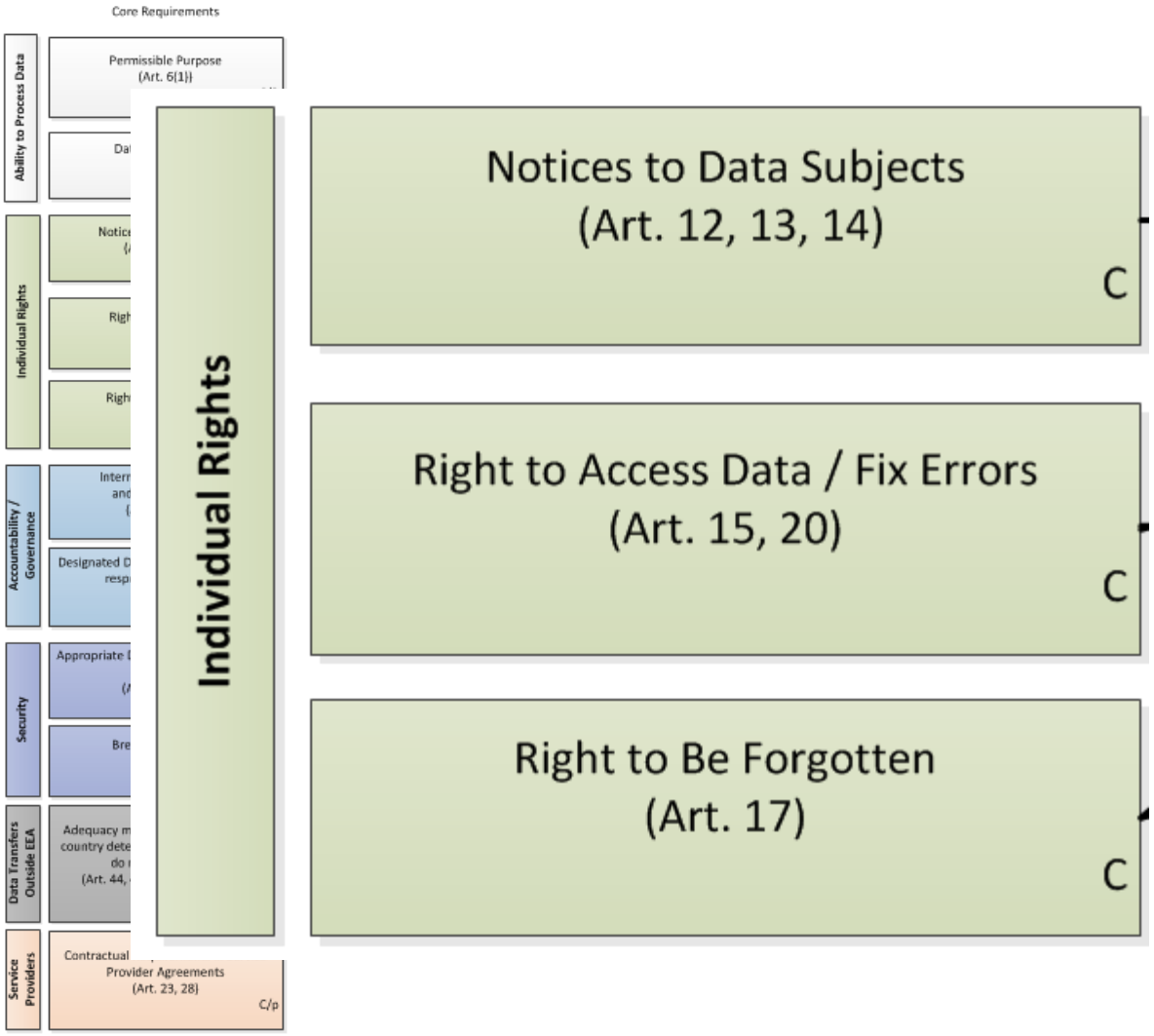
BRYAN CAVE LEIGHTON PAISNER BCLP

Level 4: What does it actually require



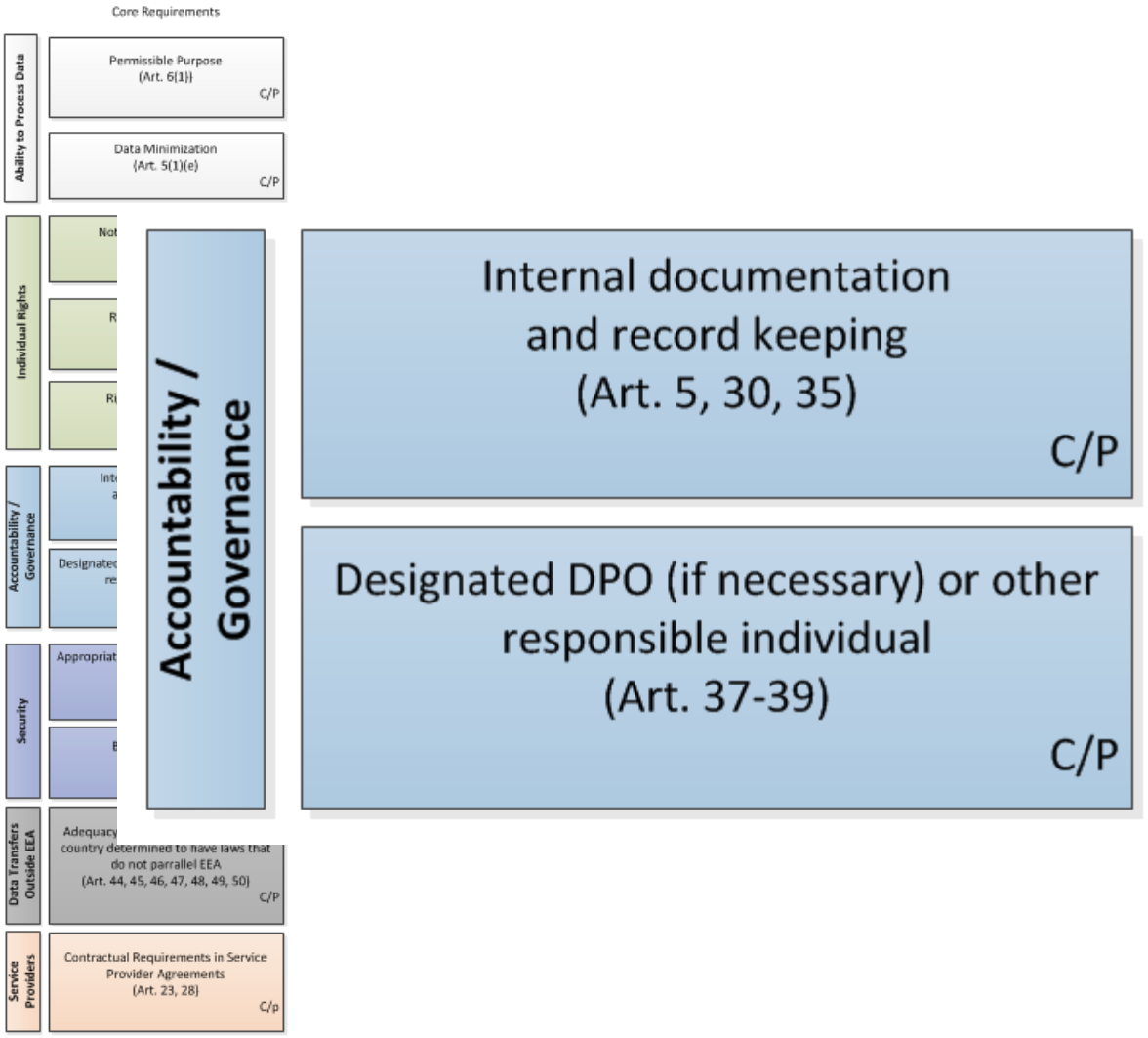
BRYAN CAVE LEIGHTON PAISNER BCLP

Level 4: What does it actually require



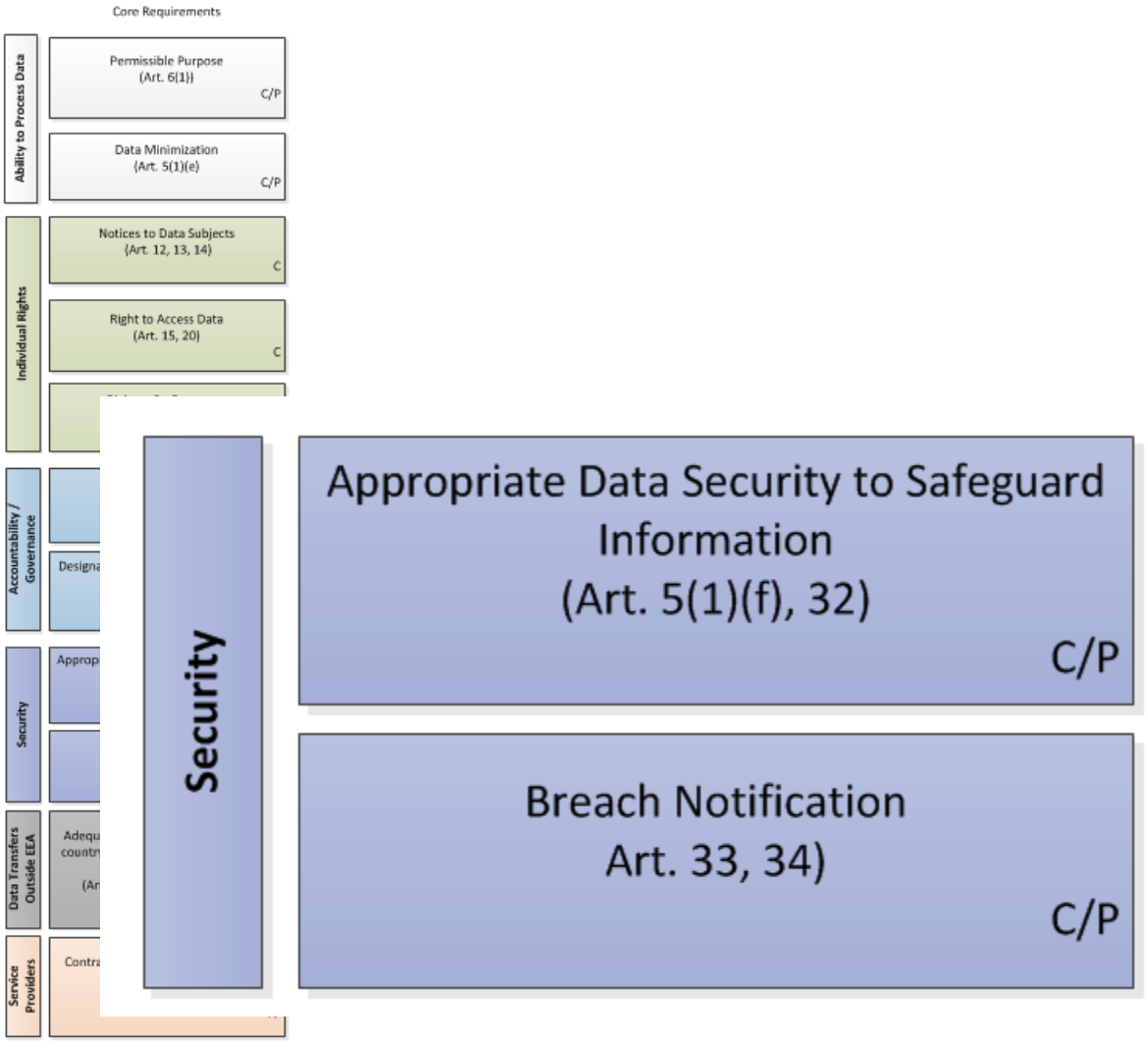
BRYAN CAVE LEIGHTON PAISNER BCLP

Level 4: What does it actually require



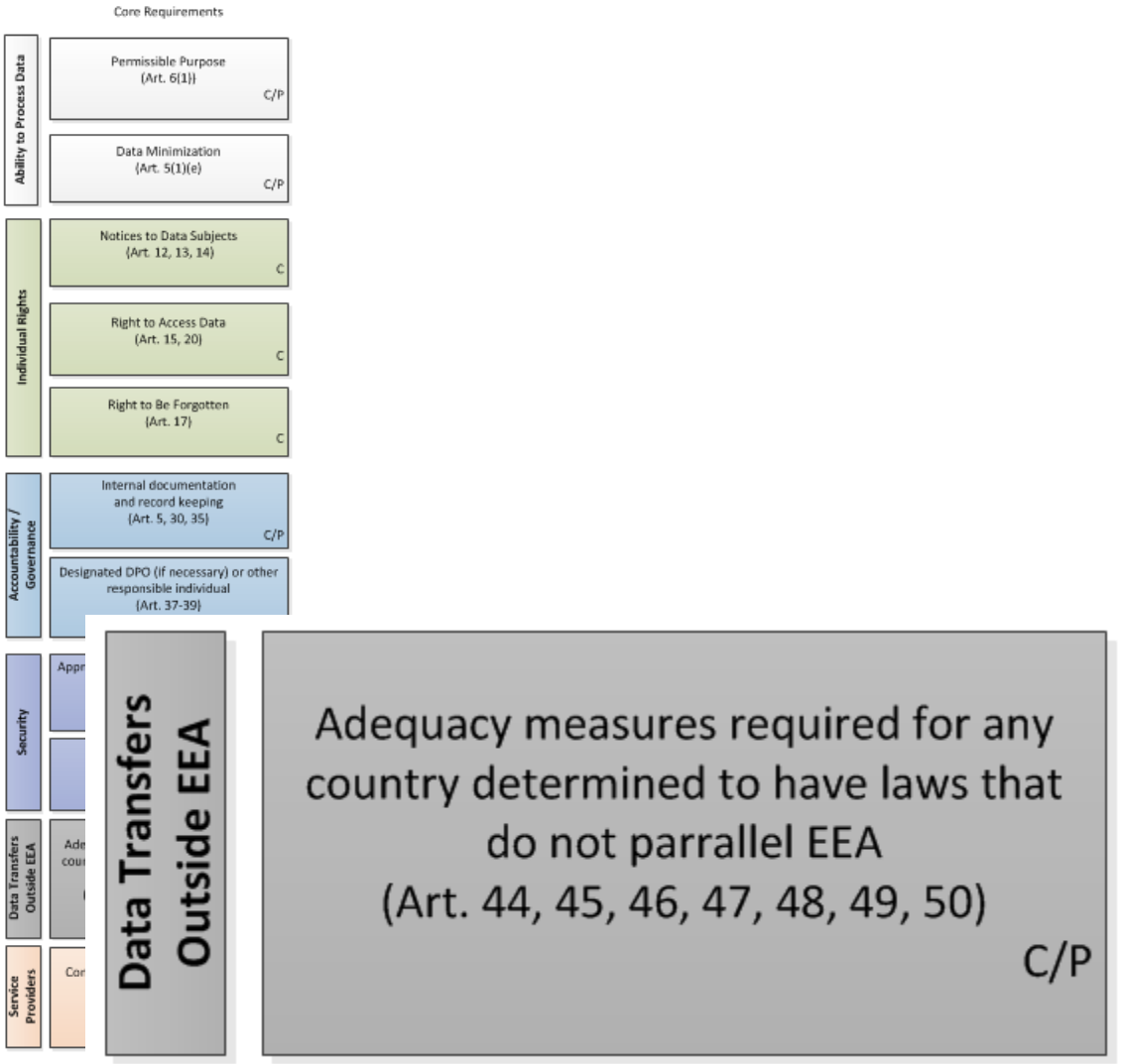
BRYAN CAVE LEIGHTON PAISNER BCLP

Level 4: What does it actually require



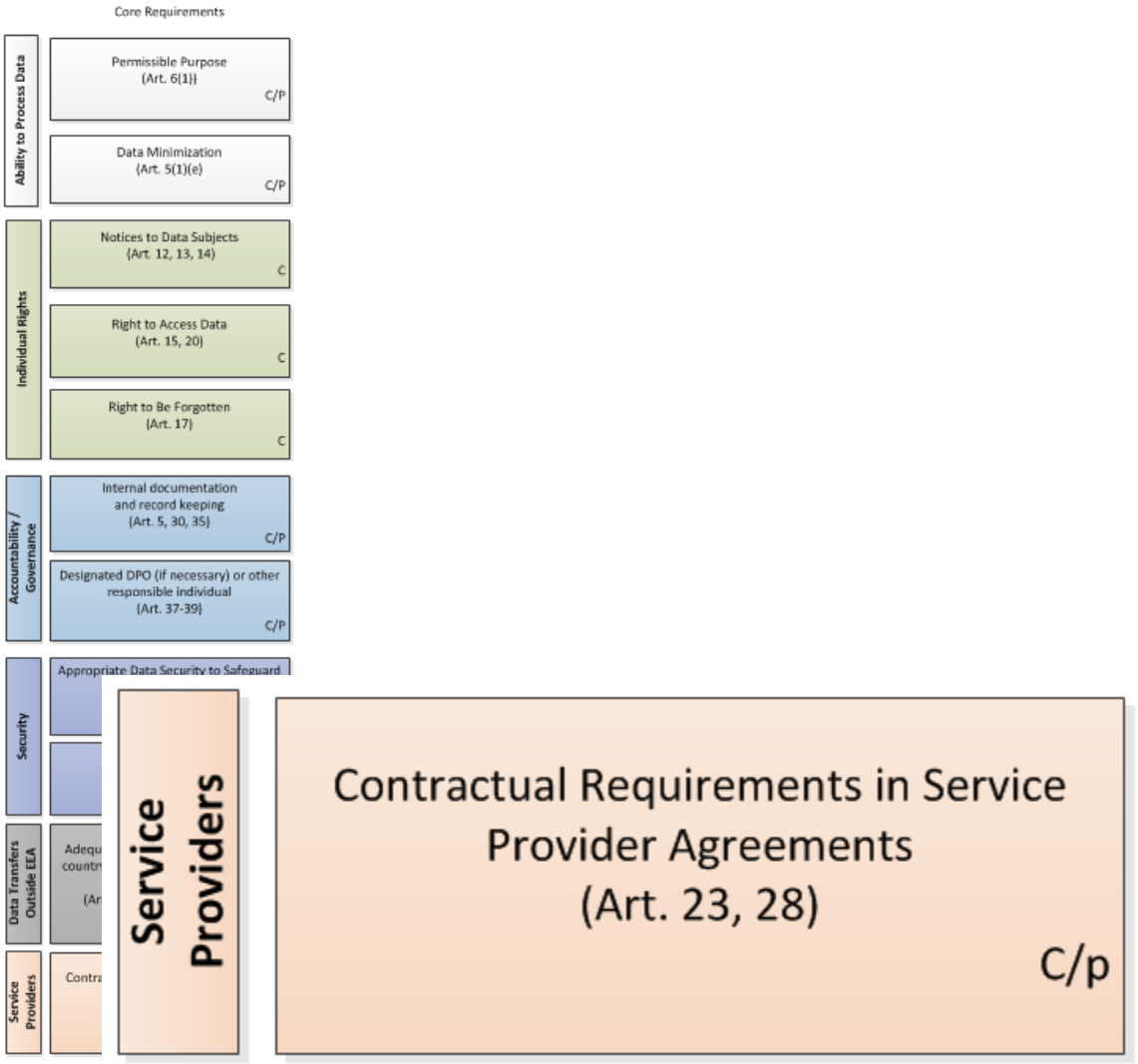
BRYAN CAVE LEIGHTON PAISNER

Level 4: What does it actually require



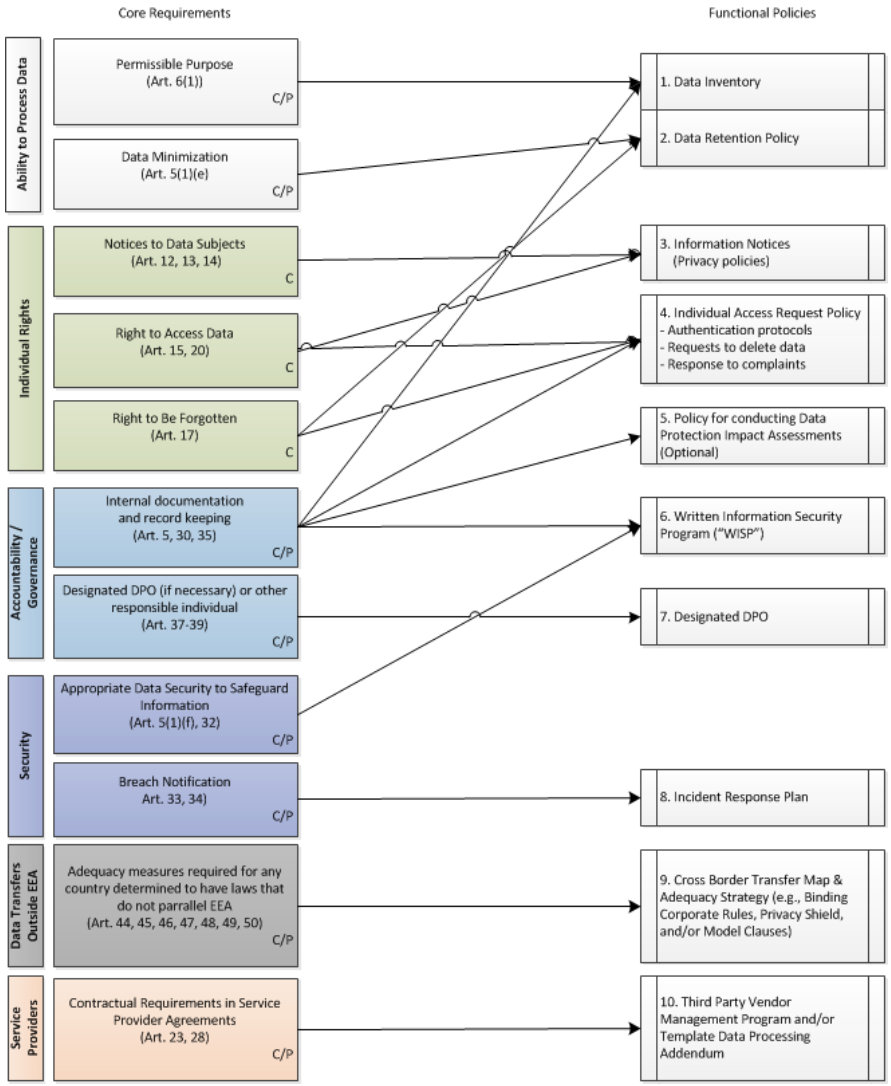
BRYAN CAVE LEIGHTON PAISNER BCLP

Level 4: What does it actually require



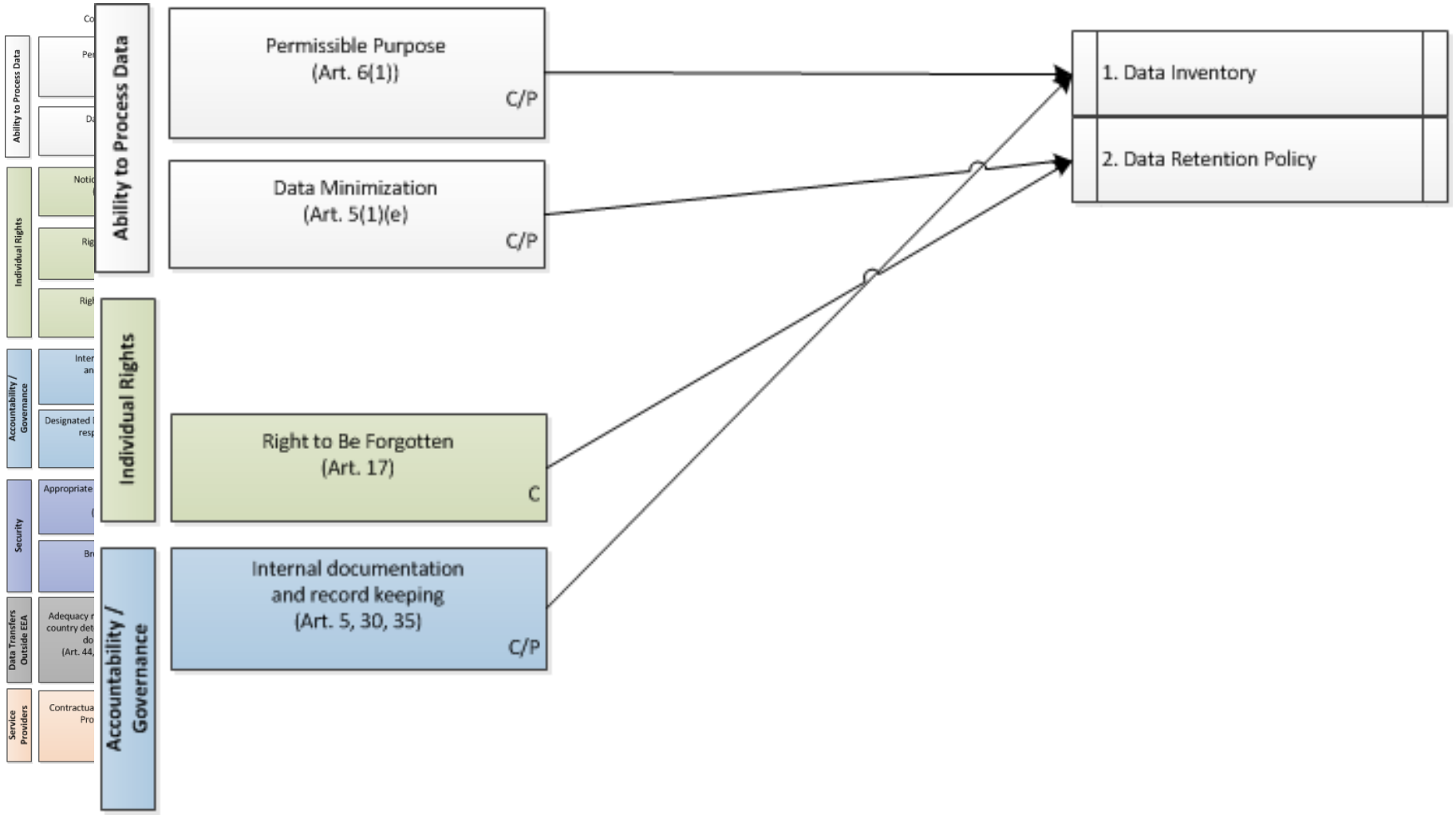
BRYAN CAVE LEIGHTON PAISNER BCLP

Level 5: Core compliance documents



BRYAN CAVE LEIGHTON PAISNER BCLP

Level 5(1): Data Inventories



BRYAN CAVE LEIGHTON PAISNER BCLP

Level 5(1): Data Inventories

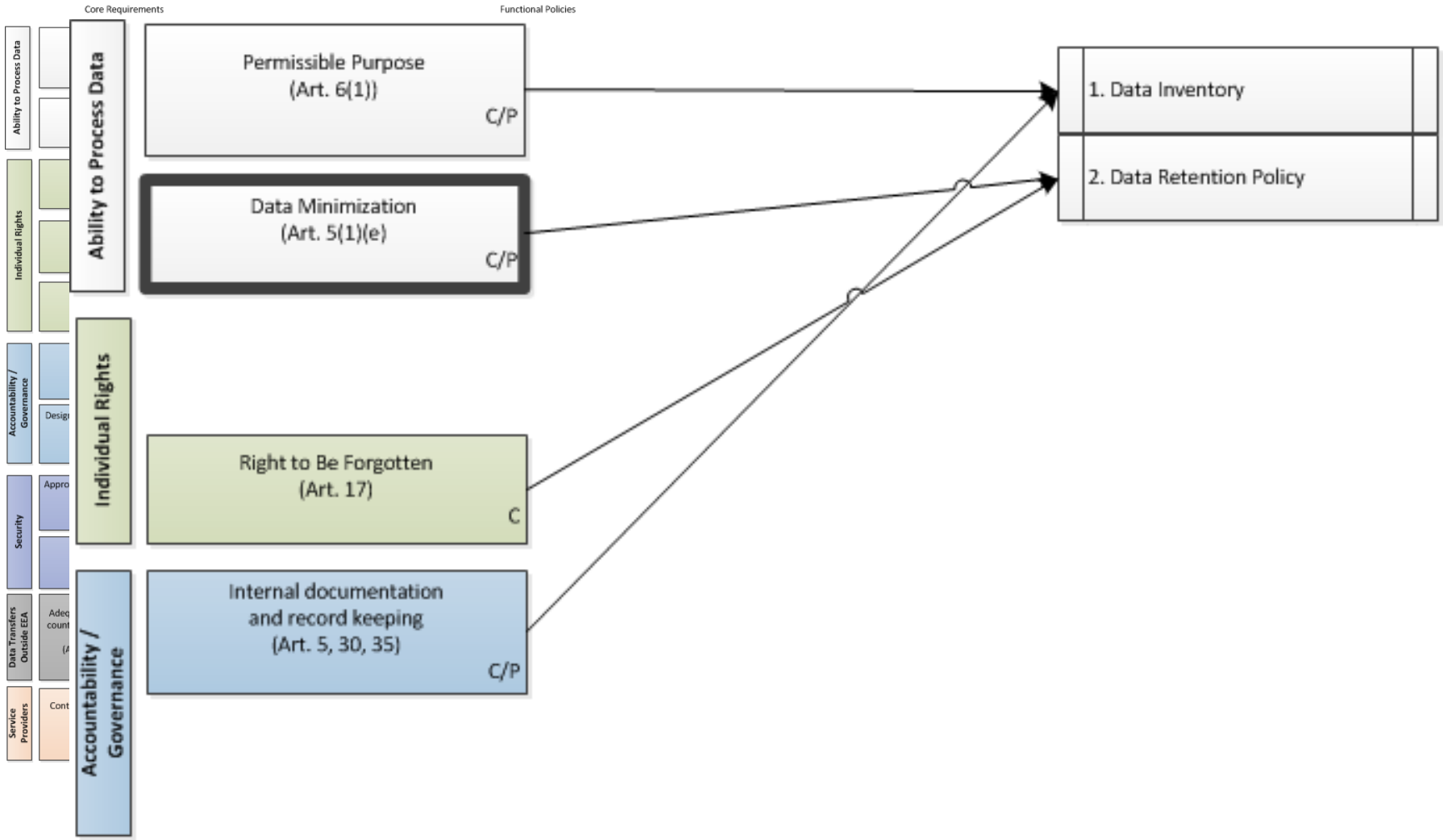
The GDPR requires that:

1. Most companies keep a record of their processing.
2. (For Controllers) the record should describe:
   A. Purpose of processing
   B. Categories of data subjects
   C. Categories of personal data
   D. Categories of recipients of that data
   E. Cross-border transfers
   F. Time limits for erasure
   G. Security measures utilized

Level 5(1): Data Inventories

- Practice pointers
  - ❑ Think about the pros- and cons- of outsourcing the creation of the data inventory.
  - ❑ Think about the pros- and cons- of creating the data inventory via questionnaires to system owners.
  - ❑ Think about the pros- and cons- of creating the data inventory via interviews.
  - ❑ Think about how to educate system owners about GDPR requirements and lingo before conducting the interview.
  - ❑ Decide if you want to use one of the supervisory authorities "safe-harbor" forms.
  - ❑ Consider a strategy for institutionalizing the upkeep of the inventory.

Level 5(2): Data retention policies



LEIGHTON PAISNER

Level 5(2): Data retention policies

The GDPR requires that:

1. You only keep data for as long as you have one of six permissible purposes.
2. Once there is no more purpose data be deleted / anonymized.

Article 5
Principles relating to processing of personal data

Personal data shall be:

…

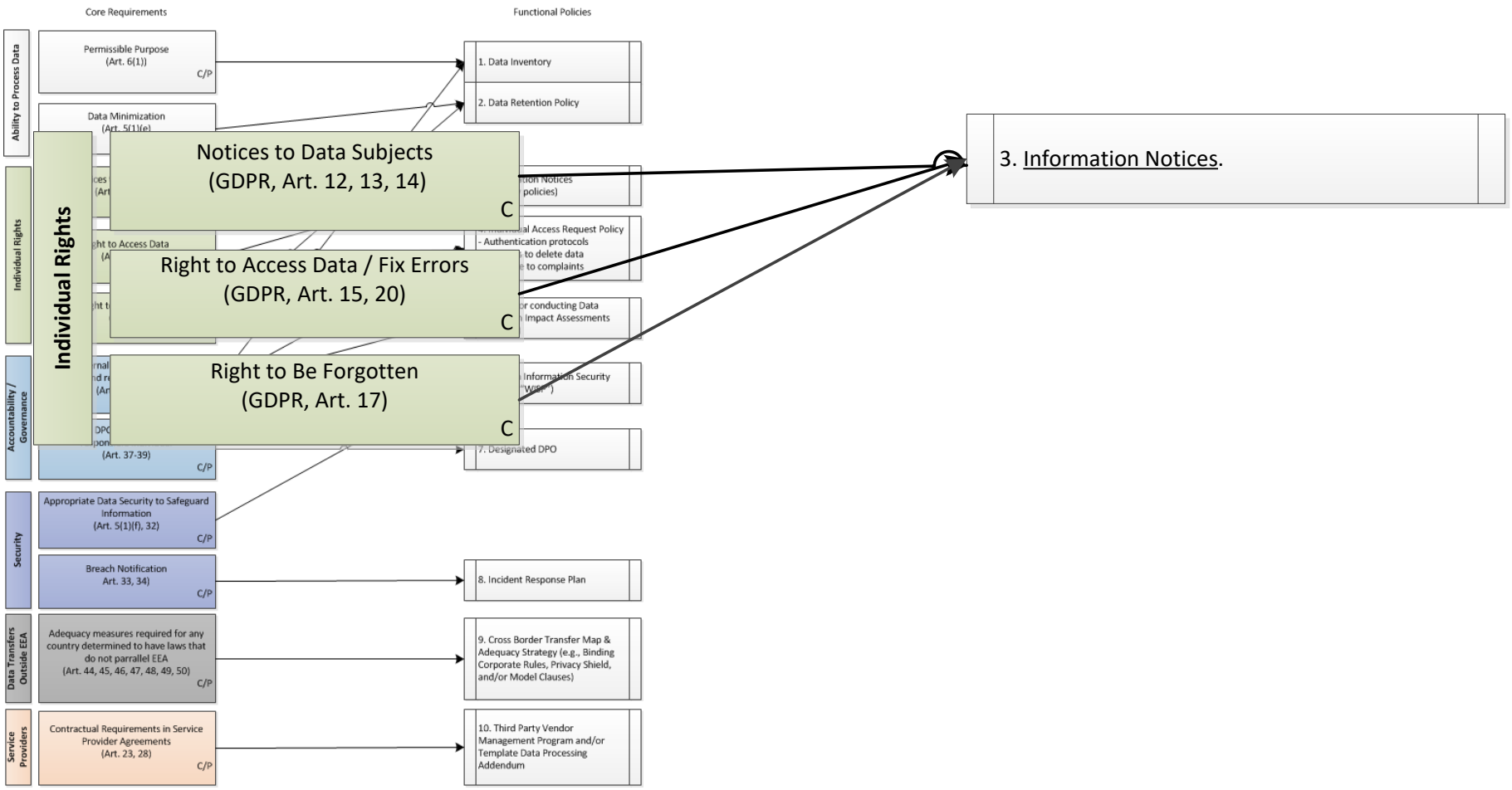
(e) kept in a form which permits identification of data subjects **for no longer than is necessary for the purposes for which the personal data are processed;** personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

Level 5(2): Data retention policies

Practice Pointers:

- Review your current retention policy / schedules to determine if they set maximums, minimums, or both.
- If maximum periods are set, and if those periods appear reasonable, focus on execution of policy.
- If maximum periods are not set, consider whether to include within the data inventory an effort to capture current retention practice, and discuss future retention needs.

Level 5(3): Information Notices



BRYAN CAVE LEIGHTON PAISNER BCLP

Level 5(3): Information Notices

- US Law:
  - Privacy policies are required in the United States in a variety of different situations.
  - What must be included in a privacy policy differs depending upon the industry, the state, and the context.
  - Depending upon the context, however, United States companies have familiarity with describing:
    - Collection
    - Use
    - Disclosure
    - Security
    - Access Rights
    - Rectification Rights
    - Erasure Rights
    - Opt-out rights
    - Where to file a complaint

Level 5(3): Information Notices

- GDPR:
  - Article 13 (Distribute privacy notice when information is collected directly from a data subject):

    "Where personal data relating to a data subject are **collected from the data subject**, the controller shall, **at the time when personal data are obtained**, provide the data subject with all of the following information . . ."

  - Article 14 (Distribute privacy notice when information is collected indirectly from another source):

    "Where personal data **have not been obtained from the data subject**, the controller shall provide the data subject with . . . information . . .

    (a) **within a reasonable period** after obtaining the personal data, but at the **latest within one month**, having regard to the specific circumstances in which the personal data are processed;

    (b) if the personal data are to be used for communication with the data subject, at the latest **at the time of the first communicatio**n to that data subject; or

    (c)if a disclosure to another recipient is envisaged, **at the latest when the personal data are first disclosed**."

Level 5(3): Information Notices

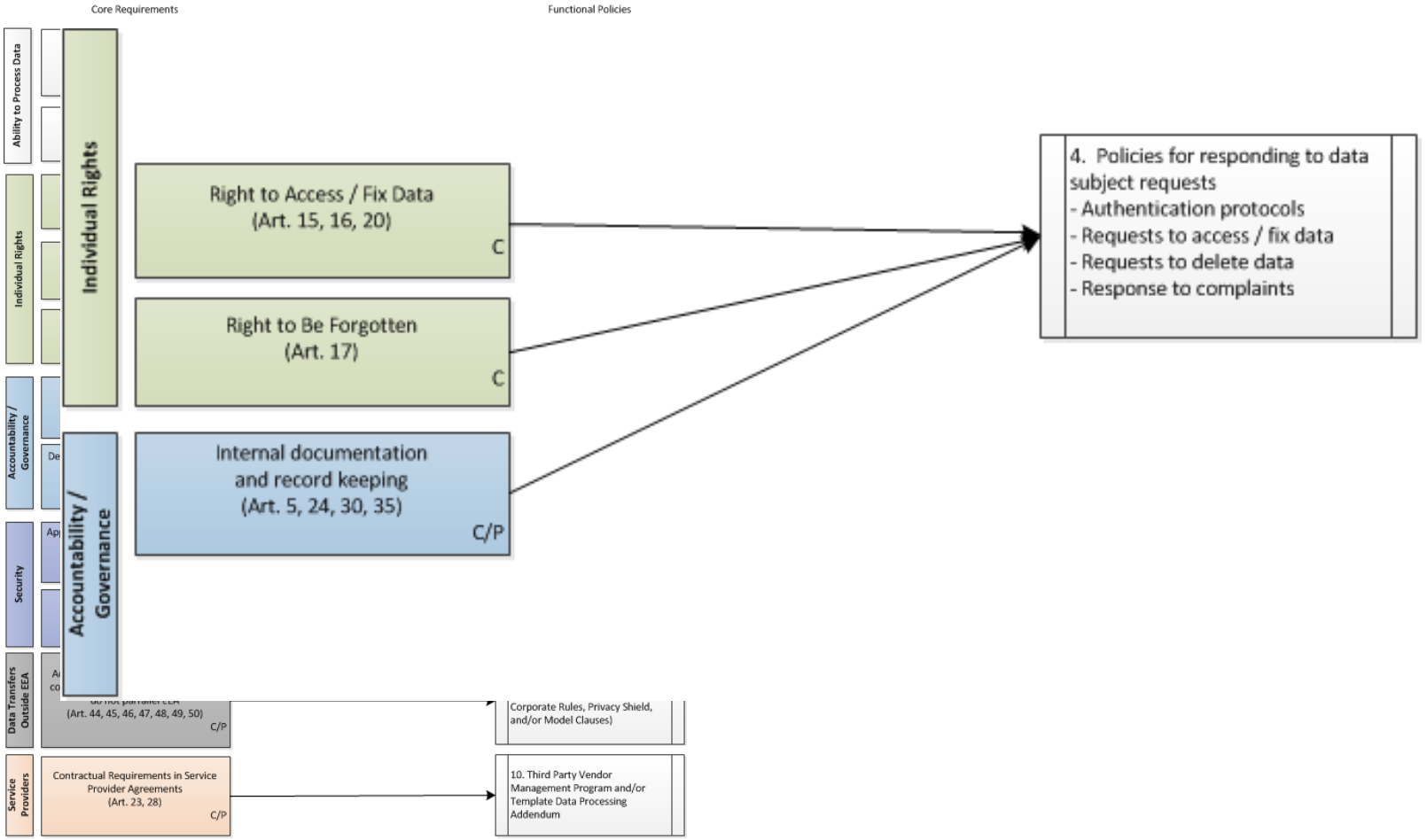
The GDPR requires the following information be included in an information notice. Provisions without an analog in United States law in red:

1. **Contact Info. Identity and contact information of the data controller, and "of the controllers' representative."**
2. **Data Protection Officer. If the controller has a data protection officer, his/her name and contact information.**
3. Description of purpose. The purposes of the processing (and the legal basis for those purposes). If one of those purposes is the "legitimate interest" of the controller, that legitimate interest must be described.
4. Description of recipients. Categories of people that will be receiving the data.
5. **Cross border transfers. If the data is going to leave the EEA that must be disclosed, as well as the "appropriate or suitable safeguards and the means by which to obtain a copy of them" for effecting such transfer.**
6. **Description of data retention period. The period for which the data will be stored, or the criteria used to determine when it will be deleted.**
7. Access Rights. Information concerning the right to request access to the information.
8. Rectification Rights. Information concerning how to ask that inaccuracies be fixed.
9. Erasure Rights. Information concerning how to ask that the data be deleted.
10. Opt-out Rights. If there is a right to opt-out of a certain use, or withdraw consent, a description of how consent can be withdrawn.
11. Complaints. A statement that the data subject has a right to lodge a complaint with a supervisory authority.
12. **Automated decision making. A disclosure if automated decision making will be occurring.**
13. **Mandatory nature of data collection A description of whether the data is required by statute or contract to be collected, as well as the possible consequences for not providing the data.**

Level 5(3): Information Notices

- Practice points
  - ❑ If a privacy policy was originally drafted under US law it may have intentionally had a limited scope (e.g., applies only to the online collection of information) that needs to be broadened for GDPR.
  - ❑ Purposes of collecting data should ideally be linked to one of the 6 “lawful basis” or “permissible purposes” identified in the GDPR.
  - ❑ Disclose all data sources (not just what you collect directly from the data subject).
  - ❑ Disclose all foreseeable situations in which information may be shared.
  - ❑ Consider discussing retention period.
  - ❑ Disclose that the data will be processed outside of the EEA.
  - ❑ Include contact information in the EEA and the US.

Level 5(4) Data Subject Request Protocols



BRYAN CAVE LEIGHTON PAISNER BCLP

Level 5(4) Data Subject Request Protocols

Article 15

Right of Access by the Data Subject

1. The data subject shall have the right to obtain **from the controller confirmation** as to whether or not personal data concerning him or her **are being processed**, and, where that is the case, **access to the personal data** and the following information:

(a) the **purposes** of the processing;

(b) the **categories of personal data** concerned;

(c) the **recipients** or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the **envisaged period for which the personal data will be stored**, or, if not possible, the criteria used to determine that period;

(e) the **existence of the right to request from the controller rectification or erasure of personal data** or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the **right to lodge a complaint** with a supervisory authority;

(g) where the personal data are not collected from the data subject, **any available information as to their source**;

(h) the **existence of automated decision-making**, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Level 5(4) Data Subject Request Protocols

Take-aways from Article 15:

A controller must:

1. Provide a copy of the personal data that they have.
2. Explain why they have the information.
3. Explain how long they intend to keep it.
4. Explain who they gave the data to (and whether the data left the EEA).
5. Provide information about fixing inaccuracies and lodging complaints

A controller does not:

1. Have to provide information about other people.

Level 5(4) Data Subject Request Protocols

Article 16
Right to Rectification

The data subject shall have the right to **obtain from the controller** without undue delay the **rectification of inaccurate personal data concerning him or her**. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Level 5(4) Data Subject Request Protocols

Article 17
Right to Erasure (Right to be Forgotten)

1. The data subject shall have the **right to obtain from the controller** the **erasure** of personal data **concerning him or her** without undue delay and the controller shall have the obligation to erase personal data without undue delay **where one of the following grounds applies**:
   - (a) the personal data are **no longer necessary** in relation to the **purposes for which they were collected** or otherwise processed;
   - (b) the data subject **withdraws consent** on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
   - (c) the data subject **objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing**, or the data subject objects to the processing pursuant to Article 21(2);
   - (d) the personal data have been **unlawfully processed**;
   - (e) the personal data have to be **erased for compliance with a legal obligation** in Union or Member State law to which the controller is subject;
   - (f) the personal data have been **collected in relation to the offer of information society services** referred to in Article 8(1).

Level 5(4) Data Subject Request Protocols

Article 17

Right to Erasure (Right to be Forgotten)

. . .

2. Where the **controller has made the personal data public** and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, **shall take reasonable steps**, including technical measures, **to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers** of any links to, or copy or replication of, those personal data.

Level 5(4) Data Subject Request Protocols

Article 17
Right to Erasure (Right to be Forgotten)

. . .

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

Level 5(4) Data Subject Request Protocols

Take-Aways Concerning Article 17:

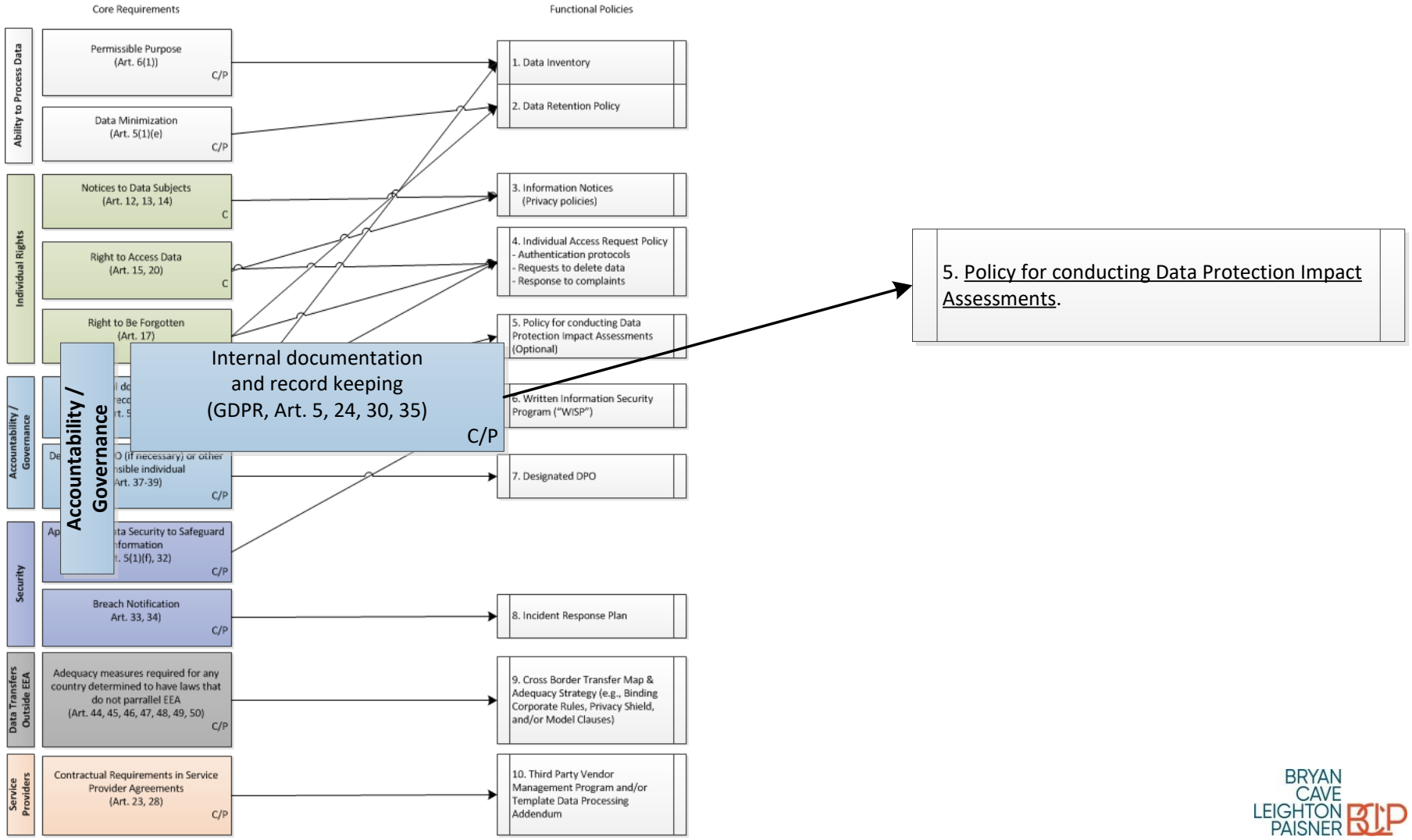
- The Right to be Forgotten is not absolute. It applies in a limited number of circumstances.
- Many of those circumstances are tautological. For example,
  - someone has a right to be forgotten if "data are no longer necessary in relation to the purposes for which they were collected." (Art. 17(1)(a).) This seems duplicative of Article 5(e) which states that data cannot be kept in an identifiable form for "longer than is necessary for the purposes for which the personal data are processed.
  - Someone has a right to be forgotten if the processing is unlawful to begin with, or if keeping the data violates a member state's laws.
- Other circumstances where the right applies revolve around withdrawing consent where the processing is based upon consent.
- Even if a situation falls under one of the enumerated circumstances, the right still does not apply if an exception kicks-in such as:
  - You are required by law to keep the data.
  - The data is necessary for freedom of information (E.g., journalism)
  - You need it to defend yourself.

Level 5(4) Data Subject Request Protocols

Practical pointers:

- ❑ Confirm the request and manage the data subject's expectations concerning time frame for a response.
- ❑ Validate the identity of the data subject.
- ❑ Evaluate the data subject's right in light of the request made. For example, if they made an erasure request, but processing is based on the performance of a contract, they may have no "right" to the erasure.
- ❑ When responding to a data subject's request, provide them with information on how to object / appeal / challenge the response.
- ❑ Consider whether internal protocols are needed in order to execute on (1) a request where the requestor has been validated, and (2) a request that is within the scope of the rights conferred by the GDPR.
- ❑ Determine what documentation to keep concerning the request and the steps that the company made to comply with the request. For example, do you keep a "right to be forgotten" request after it has been granted.

Level 5(5) Data Protection Impact Assessments



BRYAN CAVE LEIGHTON PAISNER BCLP

Level 5(5) Data Protection Impact Assessments

Article 35(1)

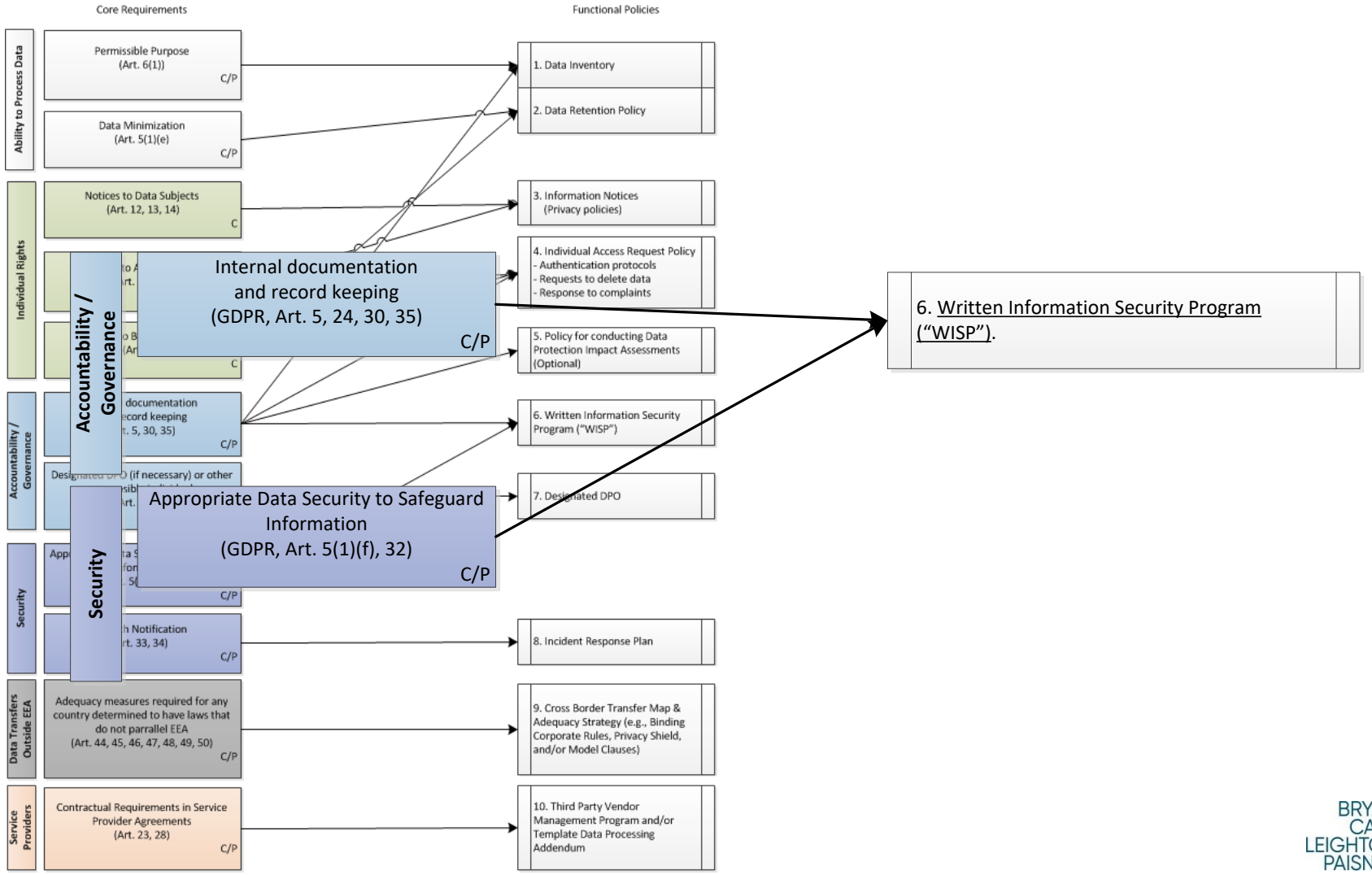
Where a **type of processing** in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is **likely to result in a high risk to the rights and freedoms of natural persons**, the **controller** shall, prior to the processing, **carry out an assessment of the impact of the envisaged processing operations on the protection of personal data**. . .

Level 5(5) Data Protection Impact Assessments

Practical pointers:

- ❑ Think about conducting a DPIA when you are doing something avant-garde with technology and data. If the market has never seen it before, there is a good chance that you should consider a DPIA.
- ❑ If there will be automated decision making with high levels of importance consider doing a DPIA.
- ❑ If you will be processing large amounts of sensitive category data consider doing a DPIA.
- ❑ If you will be monitoring people in a public space, consider doing a DPIA.
- ❑ Treat DPIA's like a legal memo: (1) issue, (2) rules, (3) analysis, (4) conclusion, (5) mitigation strategies

Level 5(6) Written Information Security Plan



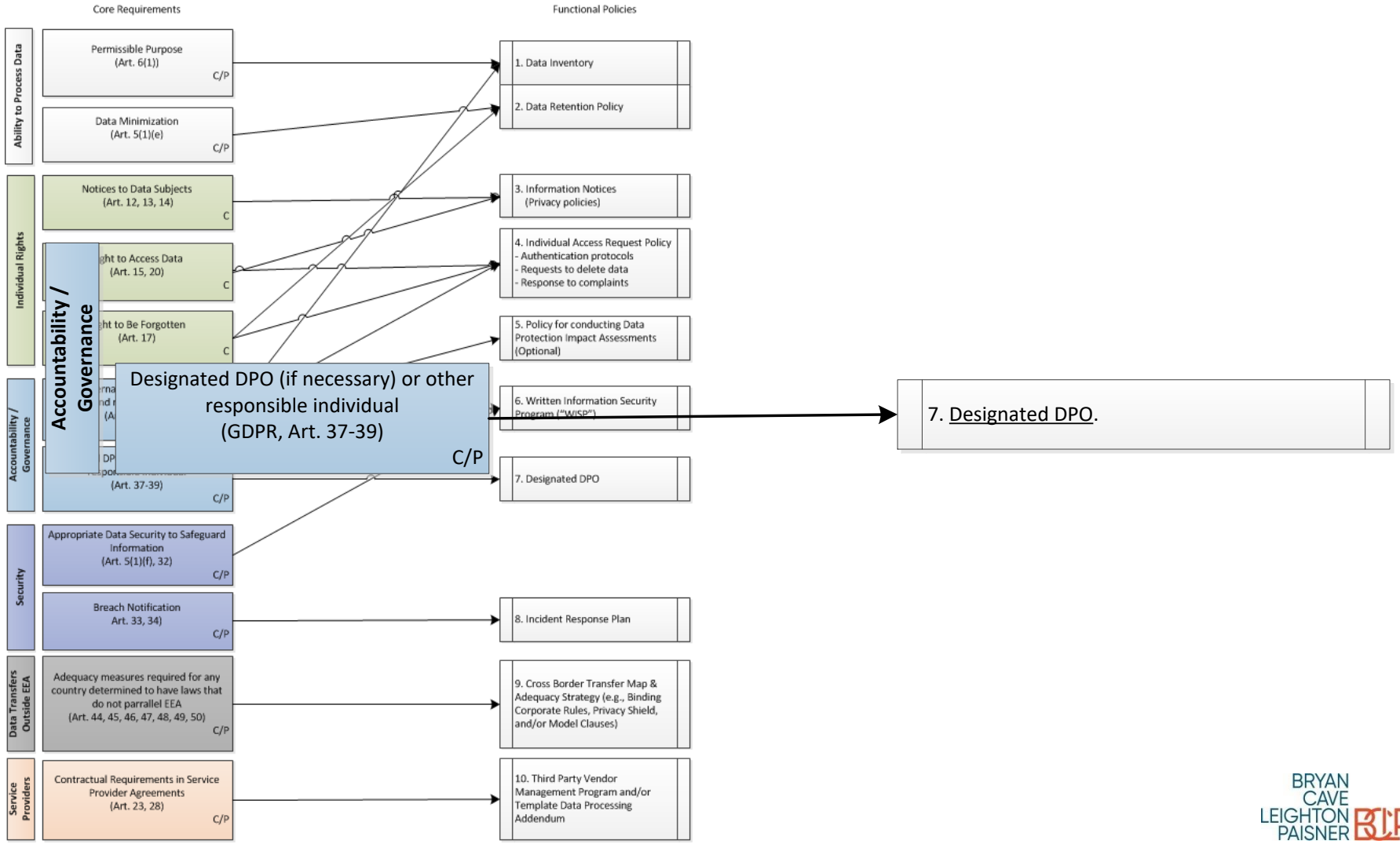
BRYAN CAVE LEIGHTON PAISNER BCLP

Level 5(6) Written Information Security Plans

Practical pointers:

- ❑ Companies that base their security process and documentation on an accepted framework (ISO, NIST, CIS) are at lower risk in terms of defending and explaining their “reasonableness” than companies with ad hoc documentation.
- ❑ Adopting off the shelf, plug-and-play policies can be incredibly dangerous if your practices don’t match the policies.

Level 5(7) Data Protection Officer



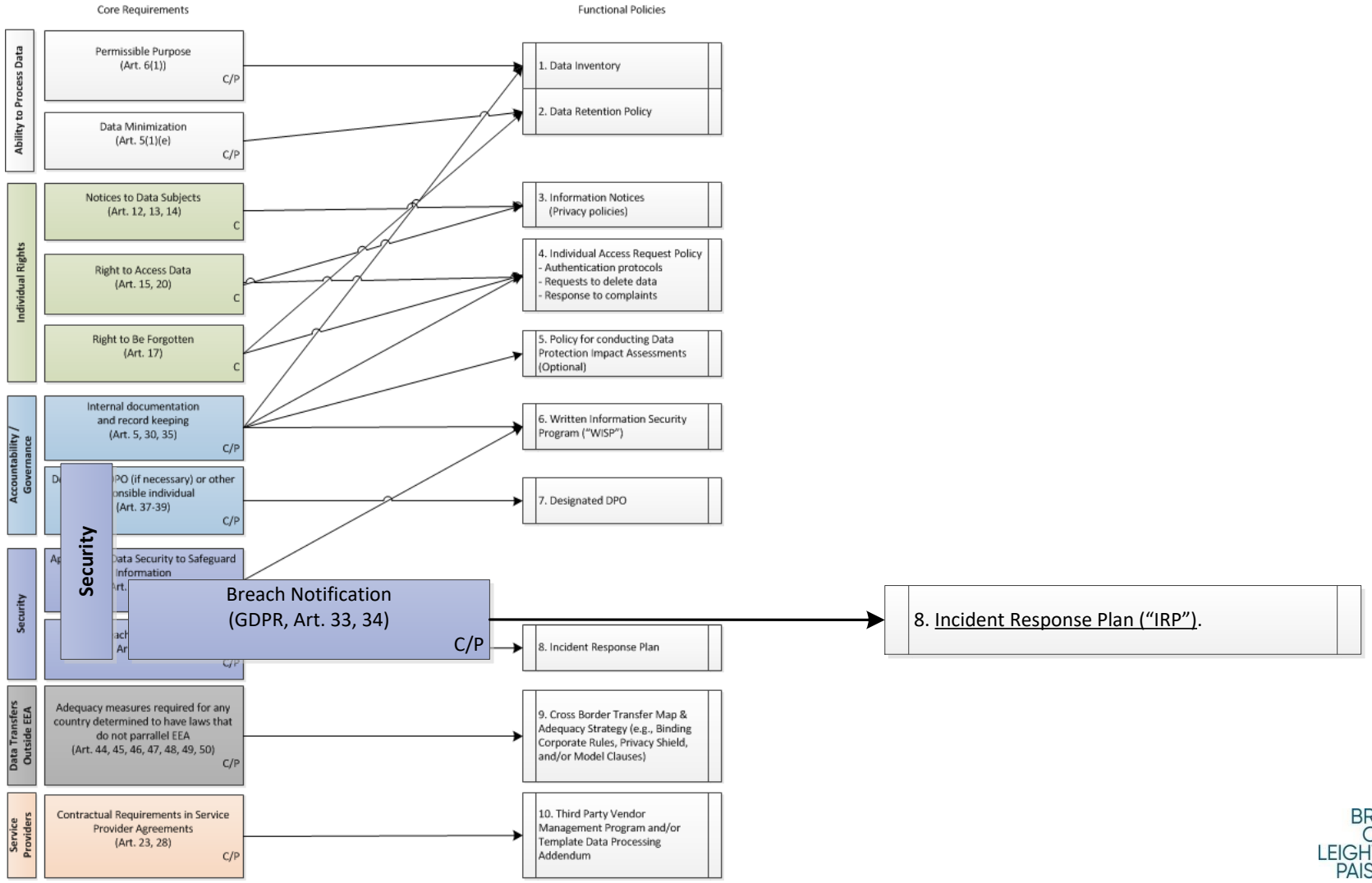
BRYAN CAVE LEIGHTON PAISNER BCLP

Level 5(7) Data Protection Officers

Practical pointers:

- ❑ Most companies are not required to appoint DPOs.
- ❑ Consider carefully whether to voluntarily appoint a DPO or, alternatively, to appoint someone with similar responsibilities but a different title (e.g., privacy officer, Chief Privacy Officer, etc.).
- ❑ Internal appointments can inadvertently create a protected position.
- ❑ External appointments can introduce various confidentiality and process issues and concerns.

Level 5(8) Incident Response Plan



BRYAN CAVE LEIGHTON PAISNER BCLP

Level 5(8) Incident Response Plan

GDPR	US
Personal Data: Any information relating to an identified or identifiable natural person.	**Personally Identifiable Information/ Personal Information**: Name + Identifier (SSN, Financial Information, Health Information, etc.)
Controller: Responsible for notice to supervisory authority and data subjects.	**Data Owner/Licensor or Covered Entity**: Responsible for notice to affected individuals and regulatory agencies.
Processor: Responsible for notice to controller.	**Licensee**: Responsible for notice to data owner/licensor or covered entity.
Supervisory Authority: Entity that receives notice, which may include concerned supervisory authority or lead authority (if cross-border).	**Regulatory Body**: Attorney General, Department of Consumer Affairs, Department of Financial Regulation, Office of Consumer Protection, or Health and Human Services.

Level 5(8) Incident Response Plan

WP29 explained, in its Opinion 03/2014, that breaches can be categorized according to the following ways:

- "**Confidentiality Breach**" – where there is an unauthorized or accidental **disclosure** of, or access to, personal data.
  - Unauthorized access or acquisition
  - Employee theft

- "**Integrity Breach**" – where there is an unauthorized or accidental **alteration** of personal data.
  - Employee tampering
  - Unauthorized access (or acquisition?)

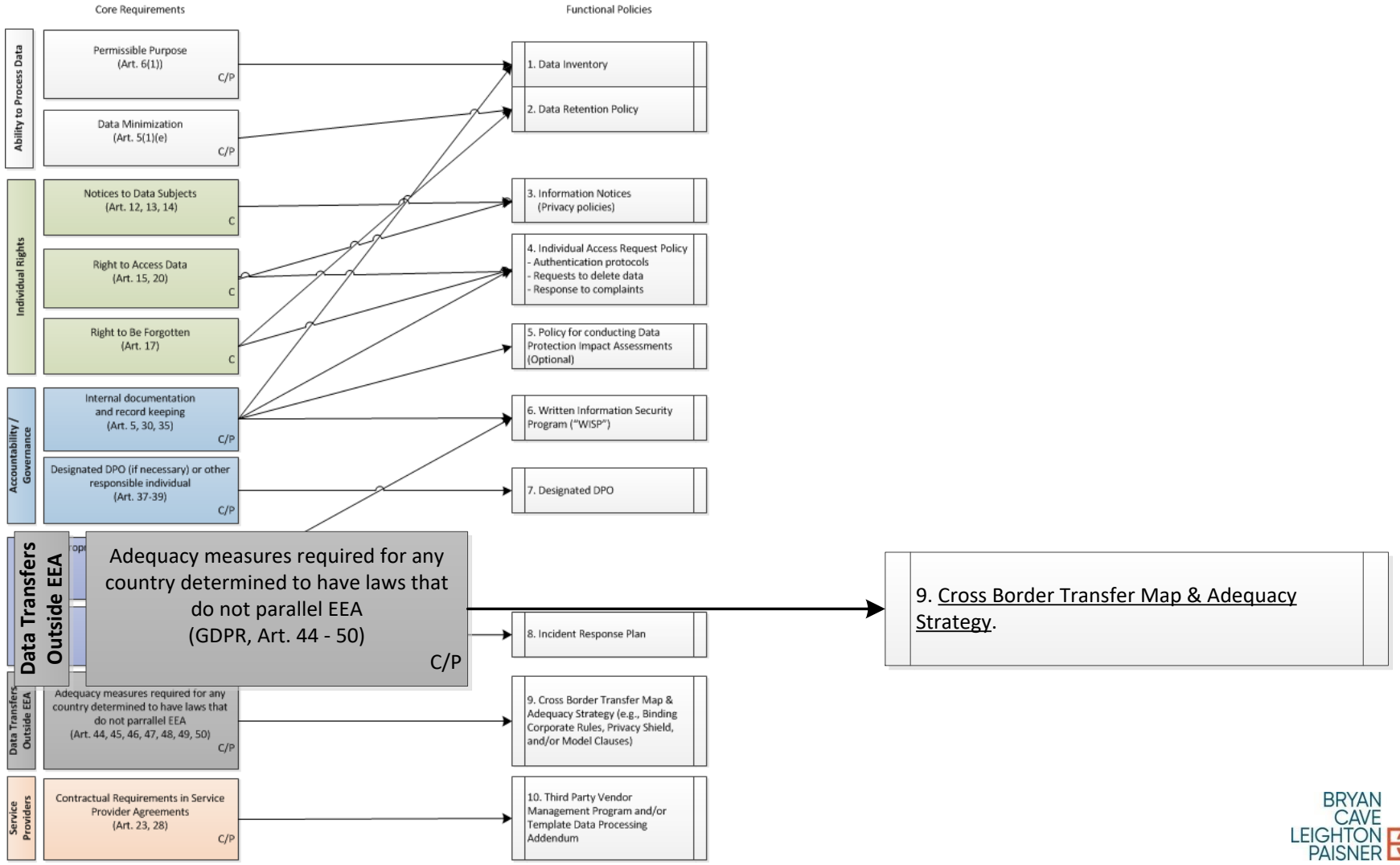
- "**Availability Breach**" – where there is an accidental or unauthorized **loss of access** to, or **destruction** of, personal data.
  - Lost laptop
  - Ransomware

Level 5(8) Incident Response Plan

Practical Pointers:

- Update definitions of “breach/incident” and “personal information” to include broader GDPR definitions.
- Pre-negotiate service agreement with forensic investigator.
- List all relevant contacts for outside counsel, forensic investigator, and competent national supervisory authority.
- Include decision making tree for determining when to notify controller, supervisory authority, and data subjects.
- Include sample notification letter and breach investigation reporting template.

Level 5(9) Cross Border Transfers



BRYAN CAVE LEIGHTON PAISNER BCLP

Level 5(9) Cross Border Transfers

GDPR requires that before personal data can be transmitted outside of the EEA, that the parties take one of three steps to ensure that the GDPR's privacy principles will follow the data:

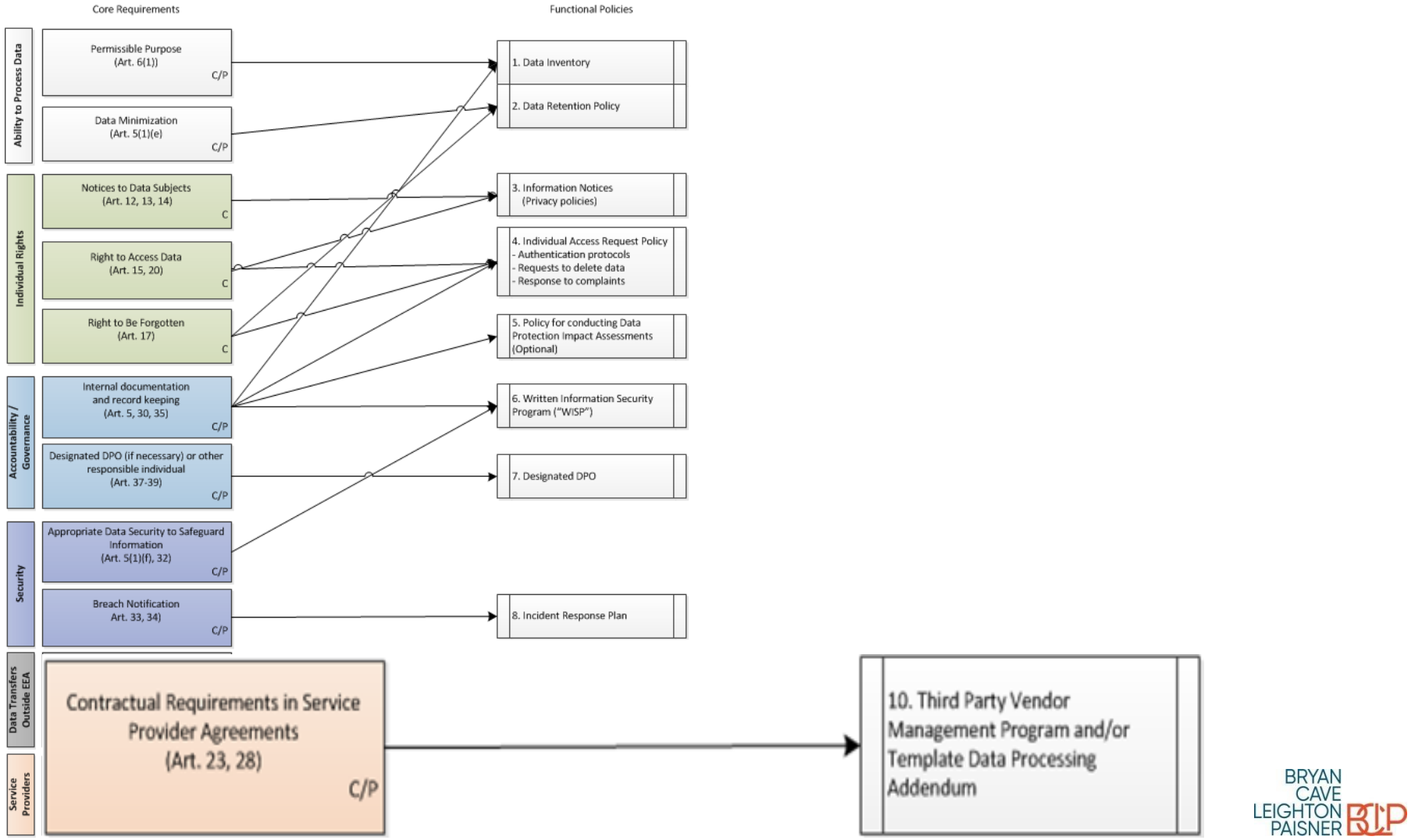
(1) Standard Contractual Clauses
(2) Binding Corporate Rules
(3) Privacy Shield

Level 5(9) Cross Border Transfers

Practice Pointers:

- ❑ Identify what personal data your organization may be exporting from Europe.
- ❑ Identify what personal data your organization may be importing from third parties that are in Europe.
- ❑ For each data flow identify an adequacy measure strategy.
- ❑ For essential data flows consider multiple strategies.

Level 5(10) Third party vendor management



BRYAN CAVE LEIGHTON PAISNER BCLP

Level 5(10) Third party vendor management

Article 28(1)
Processing Requirements

"Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."

Article 28(3)
Processing Requirements

"Processing by a processor shall be governed by a contract or other legal act under Union or Member State law that is binding on the Processor with regard to the controller . . . ." and that contains ~20 enumerated provisions.

Level 5(10) Third party vendor management

Practice Pointers:

- ❑ Identify all vendors that receive personal data.
- ❑ Validate that existing contracts (or data processing amendments) with downstream vendors comply with the GDPR.
- ❑ Have a read-to-go data processing addendum for those vendors that are not fully compliant in their contract.
- ❑ If your business provides services to other businesses review your MSA/T&C/Etc. to determine whether it complies with the GDPR.

Module 6: Biography

David Zetoony
Partner
Chair, Data Privacy & Security Team

Bryan Cave Leighton Paisner LLP
Washington, D.C. / Boulder, Colorado
202 508 6030
David.Zetoony@bclplaw.com

David Zetoony is the leader of the firm's global data privacy and security practice. He has extensive experience advising clients on how to comply with state and federal privacy, security, and advertising laws, representing clients before the Federal Trade Commission, and defending national class actions. He has assisted hundreds of companies in responding to data security incidents and breaches, and has represented human resource management companies, financial institutions, facial recognition companies, and consumer tracking companies before the Federal Trade Commission on issues involving data security and data privacy.

BRYAN CAVE LEIGHTON PAISNER BCLP

bclplaw.com